

Margaret Ellison

(602) 555-0142

Prepared October 2, 2026

Version 1 · Review by October 2, 2027

Keep this by your computer. Never write passwords in it.

If something seems wrong

Do these in order. You will not get in trouble for stopping to check.

- 1** Stop. Do not click, do not call the number on the screen, and do not send money or codes.
- 2** If someone is on the phone with you, hang up. If a warning fills the screen, turn the device off.
- 3** If money may be involved, call your bank using the number below or the one on the back of your card.
- 4** Call your family helper, Karen Ellison, at (602) 555-0142.
- 5** Write down what happened while you remember it: the time, what they said, and any phone number or website.

Your important phone numbers

Use these numbers, not ones given to you in a call, text, email or pop-up.

WHO	PHONE NUMBER	NOTES
Desert Financial Credit Union	(602) 555-0110	Checking and savings
Chase	(800) 555-0123	Credit card
Verizon (cell phone company)	1-800-922-0204	Or use the number on your bill
UnitedHealthcare (health insurance)	(800) 555-0155	Medicare Advantage plan
Dr. Patel, Estrella Family Medicine (doctor)	(623) 555-0177	
Walgreens, Litchfield Road (pharmacy)	(623) 555-0190	
Cox (internet provider)	(800) 555-0166	Internet and cable TV
Karen Ellison (daughter)	(602) 555-0142	Family helper
Emergency	911	If you are in danger or being threatened

STEP 1 OF 3

Assess

Where you stand today

Your accounts and how they are protected

A second login step means a thief needs more than your password. This list has no passwords in it, on purpose.

ACCOUNT	SECOND LOGIN STEP	NOTES
Email (Gmail)	Approve on your phone	
Desert Financial website	Text message code	
Chase credit card	Text message code	
Medicare (Medicare.gov)	Not turned on yet	
Amazon	Authenticator app code	

Your devices

How each one is set up today.

DEVICE	UNLOCKS WITH	UPDATES	BACKUP
iPhone 13	Face and 6-digit passcode	Automatic	iCloud, nightly
HP laptop	PIN	Automatic	External drive, weekly
iPad	6-digit passcode	Automatic	iCloud

Your cell phone account

Your phone number is a key to your accounts, because login codes are sent to it. Thieves try to move phone numbers to their own phones.

Cell phone company	Verizon
Your cell phone number	(602) 555-0188
To reach them	1-800-922-0204, or dial 611 from your cell phone
Protection on your number	Number lock and account PIN are both set

- ☐ Your phone company will never call or text you to ask for your PIN or a code. If someone does, hang up.
- ☐ If your phone shows "No service" or "SOS only" for more than an hour at home, call the phone company from another phone, then tell your family helper.
- ☐ Before you change your plan, add a line, or trade in a phone, you can say "I need to think about it." Then call your family helper.
- ☐ Read your phone bill each month. Call about any new line, device or charge you did not ask for.

STEP 2 OF 3

Prioritize

What you have set up, and how to use it

What you have set up

Done

- ☒ Turned on a second login step for email
- ☒ Turned on a second login step for bank and card accounts
- ☒ Turned on automatic updates
- ☒ Agreed a family code word
- ☒ Froze credit at Equifax, Experian and TransUnion

Still to do, most important first

- ☐ Set up a password manager and replaced reused passwords
- ☐ Set up a backup
- ☐ Added a trusted contact at the bank
- ☐ Removed programs and browser add-ons that were not needed
- ☐ Turn on a second login step for Medicare (Medicare.gov)

Your password manager: Apple Passwords

Built into your iPhone, iPad and Mac. It remembers a different strong password for every account, so you do not have to.

- 1** Open the Passwords app (a key icon). On an older iPhone or iPad, open Settings and tap Passwords.
- 2** Unlock it with your face, fingerprint or the passcode you use to unlock the device.
- 3** To sign in to a website: tap the username box. Your saved login appears just above the keyboard. Tap it and the name and password fill in.
- 4** To make a new account: when the site asks for a password, choose the strong password your device offers. It is saved for you.

- 5 To look something up: open Passwords and type the website's name in the search box.

Your device passcode protects every saved password. Keep it private and do not reuse it anywhere else.

If the password manager ever offers to fill in a password and then does not, stop. You may be on a fake copy of the website. Close it and call your family helper.

Your second login step

After your password, the website asks for one more thing that only you have. Here is how each kind works.

| An approval request on your phone

- 1 Sign in with your username and password as usual.
- 2 Your phone shows a message asking whether you are trying to sign in.
- 3 Tap Yes only if you are signing in right now.
- 4 If the message appears when you are not signing in, tap No. Someone may have your password. Change it, then tell your family helper.

| A code sent by text message

- 1 Sign in with your username and password as usual.
- 2 Within a minute, a text message arrives with a short code, usually six numbers.
- 3 Type that code into the website or app you just opened.
- 4 If a code arrives when you were not signing in, do nothing with it and tell your family helper.

| A code from your authenticator app

- 1 Sign in with your username and password as usual.
- 2 Open the authenticator app on your phone.
- 3 Find the name of the website in the list. Next to it is a six-digit code that changes every 30 seconds.

- 4 Type the code into the website before it changes. If it changes, just use the new one.

About login codes and approvals

A code or an approval request is a second key to your account.

Type a code only into a website or app that you opened yourself.

Never read a code to anyone on the phone. Your bank will not ask for it, and neither will I.

If your phone asks you to approve a sign-in you did not start, tap No and tell your family helper.

If you lose your phone: your backup codes are kept in the fireproof box in the hall closet. Ask your family helper to sit with you when you use them.

How to spot a scam

One of these is a warning. Two or more is almost certainly a scam.

- ☐ Someone contacts you first, by phone, text, email or pop-up, about a problem you did not know you had.
- ☐ They say you must act right now, or something bad will happen.
- ☐ They ask you to keep it secret from your bank, your family or anyone else.
- ☐ They want payment by gift card, wire transfer, cryptocurrency, cash in the mail or a payment app.
- ☐ They ask for a code that was just sent to your phone or email.
- ☐ They ask to connect to your computer or phone, or to install a program so they can 'help'.
- ☐ They say they are from your bank, Microsoft, Apple, Medicare, Social Security, the IRS or the police.
- ☐ A message or pop-up tells you to call a phone number it gives you.

What to do every time

- 1 Stop. Real problems can wait ten minutes. Scams cannot.
- 2 Hang up or close the message. You are not being rude.

- 3 Look up the phone number yourself, on the back of your card or on a statement, and call that.
- 4 Never read a login code to anyone. Type it only into a website or app you opened yourself.
- 5 When in doubt, call your family helper before you do anything else.

Your family has a code word. It is not written here. Anyone who calls saying they are family and need money must say it. If they cannot, hang up.

STEP 3 OF 3

Adjust

Keeping it current

Your ten-minute monthly check

Pick a day, such as the first of the month, and tick these off.

- ☐ Read your bank and card statements. Call the bank about any charge you do not recognize.
- ☐ Install updates when your phone or computer offers them, then restart the device.
- ☐ Check that your backup ran this month.
- ☐ Delete emails and texts from senders you do not know, without tapping any links.
- ☐ Tell your family helper about anything that seemed odd, even if you handled it.

Once a year

- ☐ Get your free credit reports at AnnualCreditReport.com and look for accounts you did not open.
- ☐ Ask your bank to confirm the trusted contact on your accounts.
- ☐ Go through this playbook with your family helper, and print the new version.

This playbook has a review date

Phone numbers, websites and scams change. Review this playbook by October 2, 2027.

Before then, go through it with your family helper and print a new version.

Also update this playbook if you get a new phone or computer, change banks, or move.

Where to report fraud and get help

Call your bank first if money is involved. A report also strengthens a bank dispute.

WHO	PHONE	WEBSITE	USE IT FOR
Federal Trade Commission	1-877-382-4357	ReportFraud.ftc.gov	Report any scam
Identity theft recovery (FTC)	1-877-438-4338	IdentityTheft.gov	Someone used your name or Social Security number

WHO	PHONE	WEBSITE	USE IT FOR
FBI Internet Crime Complaint Center		ic3.gov	Online fraud, especially if money was lost
National Elder Fraud Hotline	1-833-372-8311		Help for adults 60 and over, U.S. Department of Justice
AARP Fraud Watch Helpline	1-877-908-3360	aarp.org/fraud	Talk to a trained volunteer
Equifax	1-888-298-0045	equifax.com	Freeze or unfreeze your credit
Experian	1-888-397-3742	experian.com	Freeze or unfreeze your credit
TransUnion	1-800-916-8800	transunion.com	Freeze or unfreeze your credit
Social Security fraud line	1-800-269-0271	oig.ssa.gov	Scams using Social Security's name
Medicare	1-800-633-4227	medicare.gov	Medicare card or billing fraud
IRS	1-800-829-1040	irs.gov	Check whether a letter or bill from the IRS is real
IRS identity theft line	1-800-908-4490	irs.gov/identitytheft	Someone filed a tax return in your name
Treasury Inspector General (TIGTA)	1-800-366-4484	tigta.gov	Report someone pretending to be the IRS
Arizona Attorney General	602-542-5763	azag.gov	Consumer fraud complaints in Arizona
Arizona Adult Protective Services	1-877-767-2385		Someone is exploiting a vulnerable adult
Maricopa County Sheriff, non-emergency	602-876-1011		File a police report

Phone numbers last checked October 2026.

For your family helper

Karen Ellison, this page is for you.

- ☐ Be the first call. If something seems wrong, your relative should be able to reach you without feeling judged.
- ☐ Never ask for passwords by phone, text or email. If you need to help with an account, do it together, in person or on a video call.
- ☐ Agree on a family code word. Anyone who calls claiming to be family and asking for money must know it.
- ☐ Know where this playbook and the password manager's emergency sheet are kept.
- ☐ If money has left an account, the bank's fraud line comes first, then the reports listed in this playbook.

Rules that never change

Nobody honest asks for your passwords or for the codes sent to your phone.

Nobody honest asks to be paid in gift cards, wire transfers or cryptocurrency.

If a caller says they are from your bank, a company or the government, hang up and dial the number in this playbook yourself.

Want someone to check this with you? Jeff Cady Security

(206) 849-7494 · jeff@jcady.org · security.jcady.org